Transkript Podcastfolge: Souveräne Clouds

Ein Beitrag von Nicolas John, Johannes Müller, Johanna Voget, Klaus Palenberg, 2. August 2023

Beschreibung:

Digitale Souveränität ist zum politischen Entwicklungsziel geworden. Gerade im Bereich des Cloud-Computings steht häufig in Frage, wie Kontrolle über Daten effektiv ausgeübt werden kann. In dieser Folge von Weggeforscht stellen die Wissenschaftlichen Mitarbeiter:innen Johanna Voget und Johannes Müller das Positionspapier der DSK zu Souveränen Clouds vor und diskutieren die hierin aufgestellten Kriterien.

Transkript

00:00:06 John

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN.

00:00:15 Voget

Hallo und herzlich Willkommen zu einer neuen Ausgabe von „Weggeforscht“. Heute am Mikrofon sind für Sie mein Kollege Johannes Müller und ich, Johanna Voget.

00:00:23 Müller

Auch von mir ein herzliches Willkommen.

00:00:25 Voget

Wir wollen heute über das Thema Cloud-Computing sprechen oder genauer noch über souveräne Clouds und die Stellungnahme der DSK hierzu. Aber zunächst einmal wie gewohnt: Was gibts neues?

00:00:39 Palenberg

1,2 Milliarden Euro Strafe gegen Meta wegen Verstößen gegen europäische Datenschutzregeln. Gegen den Facebook-Konzern Meta wurde die mit einer Höhe von 1,2 Milliarden Euro bislang höchste in Europa verhängte Strafe wegen Verstößen gegen Datenschutzregeln ausgesprochen. Hintergrund der Entscheidung ist die rechtswidrige Vermittlung von Nutzerdaten durch Facebook auf Server in die USA. Neben der Geldstrafe wurde der Konzern außerdem dazu aufgefordert, künftig keine weiteren Daten in die USA mehr zu übermitteln, hierfür bleibt dem Konzern eine fünfmonatige Umsetzungsfrist.

Fünfjähriges Jubiläum der DSGVO. Seit dem 28. Mai 2018 beansprucht in der gesamten Europäischen Union Geltung und bis heute beschäftigen ihre Regelungen Datenschützer täglich. Die Datenschutzgrundverordnung, kurz DSGVO, feiert ihr fünfjähriges Bestehen. Neben der Verunsicherung und einer gefürchteten Überregulierung durch die neuen europäischen Datenschutzregelungen wurde jedoch ebenso ein einheitliches Schutzniveau in der Europäischen Union geschaffen, welches zu einer Stärkung und effektiveren Durchsetzung der betroffenen Rechte geführt hat. Doch auch nach 5 Jahren der Anwendung bleiben Unklarheiten und treten immer wieder neue Herausforderungen, wie zum Beispiel die künstliche Intelligenz auf den Plan, denen sich die DSGVO stellen muss.

00:01:48 Voget

Ja, wie gerade angekündigt, möchten wir uns heute mit der Stellungnahme der DSK zur souveränen Cloud-Nutzung beschäftigen. Aber vorweg, bevor ich jetzt hier diesen Begriff noch drei Mal nenne, willst du vielleicht noch einmal erklären, was ist die DSK überhaupt und was macht sie?

00:02:01 Müller

Ja gerne. Also die DSK als Name steht für die Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden und wie der Name schon sagt, handelt es sich dabei um ein Gremium, das sich aus den verschiedenen Datenschutzaufsichtsbehörden des Bundes und der Länder zusammensetzt. Und die veröffentlichen dann häufig Entschließungen oder Orientierungshilfen zu bestimmten, meist datenschutzrechtlichen Themen. Den Veröffentlichungen wird in der Regel ein recht hohes Gewicht beigemessen, da sie nun mal von denjenigen Behörden stammen, die selbst mit der Überwachung des Datenschutzes beauftragt sind.

00:02:30 Voget

Okay ja danke für die Erklärung schon mal. Und jetzt hat sich eben diese Datenschutzkonferenz mit der Souveränität von Cloud-Diensten auseinandergesetzt. Das ist ja auf jeden Fall ein hoch relevantes Thema, was die meisten von uns betrifft, weil jeder benutzt mittlerweile eine Cloud und speichert seine Daten nicht mehr auf ja nur Speichergeräten, sondern eigentlich ja eben halt in der Cloud. Und ja, Cloud Computing vielleicht vorweg beschreibt ja das Bereitstellen von Computerressourcen, also Datenspeichern über das Internet, so dass Anwender von Cloud Diensten ihre digitalen Infrastrukturen auslagern können. Was ist denn jetzt aber mit diesen souveränen Clouds gemeint? Was ist die Besonderheit bei denen?

00:03:09 Müller

Genau also die Thematik von souveräne Cloud hängt natürlich eng mit den Risiken zusammen. Die bei der Nutzung von Clouds entstehen. Und dadurch, dass man seine eigenen IT-Ressourcen über das Internet ausgelagert und jetzt nicht mehr bei sich zu Hause vielleicht auf der Festplatte hat, verliert man natürlich in gewisser Weise auch einen Teil der Kontrolle über die eigenen Daten. Da die Daten nicht auf dem Server liegen, ist es schwieriger festzustellen, wer tatsächlich Zugriff auf diese Daten hat und wie ein solcher Zugriff als die Datenverarbeitung ausgestaltet ist. Und die Risiken werden dann natürlich noch einmal deutlich größer, wenn die Server zum Beispiel außerhalb von der EU stehen und daher gegebenenfalls europäische Datenschutzstandards nicht unmittelbar gelten. Das hängt natürlich von den Einzelfällen dann ab. Und auf diesen Risiken aufbauend bedeutet Souveränität im digitalen Raum, also es zum Beispiel Stellungnahme, dass Individuen und Institutionen im Stande sind, ihre Rollen selbstständig, selbstbestimmt und sicher ausüben zu können.

00:04:01 Voget

OK, also die DSK betrachtet digitale Souveränität bei Clouds und das Ganze aus datenschutzrechtlicher Perspektive jetzt in ihrer Stellungnahme.

00:04:09 Müller

Ganz genau, es ist in gewisser Weise auch die Aufgabe der DSK, dass sie sich vor allem mit datenschutzrechtlichen Themen beschäftigen und deshalb betont die Stellungnahme, dass eine souveräne Cloud alle Vorgaben des Datenschutzrechts einhalten muss. Das alleine genügt natürlich noch nicht. Darüber hinaus muss eine souveräne Cloud die zugrundeliegenden Probleme rund um die

Datenkontrolle vor allem grundlegend und nachhaltig lösen. Also es kann sein, dass noch deutlich höhere Anforderungen gelten müssen, als wirklich die Einhaltung des Datenschutzrechtes, also man muss mehr machen als sich einfach nur rechtlich konform verhalten.

00:04:40 Voget

OK, ja genau. Und in der Stellungnahme werden ja dazu auch konkret unterschiedliche Kriterien genannt, anhand derer die Anbieter von Cloud Diensten und auch die Anwender selbst feststellen können, ob ein bestimmter Cloud Dienst im Einzelnen diese Anforderungen an die digitale Souveränität erfüllt, richtig?

00:04:55 Müller

Genau. Und hierbei wird dann zwischen muss- und soll- Kriterien entschieden. Erstere müssen Clouds erfüllen, um als souverän zu gelten, und letztere sind lediglich Empfehlungen.

00:05:05 Voget

Okay, dann lass uns doch mal einsteigen und ein bisschen anschaulich für die Zuhörer erläutern, was für Vorgaben das denn im Einzelnen sind. Da gibt es auf jeden Fall das Kriterium der Nachvollziehbarkeit durch Transparenz. Der datenschutzrechtliche Transparenzgrundsatz ist ja in Artikel 5 Absatz 1 lit. a der DSGVO auch selbst normiert und danach hat eine Verarbeitung personenbezogener Daten in einer für die betroffene Person nachvollziehbaren Weise zu erfolgen. Klingt jetzt alles kompliziert. Was bedeutet das konkret für souveräne Clouds?

00:05:34 Müller

Genau also in ähnlicher Weise bedeutet das dann im Grunde auch, dass die Datenverarbeitung durch den Clouddienst, durch den Anbieter in einer Weise zu erfolgen hat, die selbst für die Anwender nachvollziehbar ist. Das heißt, der Cloud Dienst muss stets imstande sein, nachzuweisen, dass die Verarbeitung vollkommen datenschutzkonform erfolgt. Und dazu nennt die Stellungnahme unterschiedliche Kriterien, auf die sich die Transparenz beziehen soll. Hierauf wollen wir aber gar nicht ganz genau im Detail eingehen. Das würde, glaube ich, den Rahmen des Podcast sprengen. Aber beispielsweise kann zum Beispiel gesagt werden, das bereits vor Vertragsschluss eine Dokumentation vorliegen soll, über externe Komponenten, die eingesetzt werden und auch Dienstleistungen. Und ebenso soll die Transparenzpflicht sich auf verfügbare Schnittstellen und die Möglichkeiten des Daten Exports beziehen. Und aus Gründen der Transparenz sagt die Stellungnahme, dass besonders empfehlenswert ist, dass Open Source Software und offene Standards eingesetzt wird.

00:06:28 Voget

Okay ja, das klingt ja auch alles nach Transparenz. Und was meint dann die Voraussetzung der Kontrollierbarkeit ihrer Nutzung, was ist damit gemeint?

00:06:38 Müller

Genau, also so ganz kurz zusammengefasst bedeutet dies, dass betroffene Person ihre Datenhoheit wahren können sollen, also dass die Kontrolle darüber haben, wer ihre Daten verarbeitet und wie eine solche Datenverarbeitung aussieht.

00:06:51 Müller

Und dies wird insbesondere sichergestellt, indem die Anbieter der Cloud personenbezogene Daten ausschließlich im Rahmen von konkreten Weisungen, also Weisungen von den Anwendern, verarbeiten und neben unterschiedlichen Punkten empfiehlt die Stellungnahme beispielsweise, dass bei der Einschaltung von Unterauftragsverarbeitern die Anwender selbst möglichst weitgehend auf diese einwirken sollen und auch einzelne Unterauftragsverarbeiter abwählen können sollen. Und zu dem Kriterium der Datenhoheit zählt die DSK auch, dass Zugriffsmöglichkeiten der Behörden von Drittländern verhindert werden sollen. Wir können das Ganze vor allem aus der Problematik rund um die Privacy Shield-Abkommen mit den USA, genau, und hier wird gesagt, das es zur Verhinderung von Datenzugriffen in der Regel nicht ausreicht, dass vertragliche Maßnahmen lediglich getroffen werden. Und natürlich werden noch weitere Punkte rund um die Datenkontrolle aufgelistet, aber um Sie, liebe Hörerinnen und Hörer nicht zu langweilen, wollen wir vielleicht nur noch einen Punkt nennen. Der ist recht interessant, da hier die Stellungnahme deutlich über die Anforderungen der DSGVOhinausgeht. Also DSGVO sieht die Möglichkeit vor, dass eine Übertragung von personenbezogenen Daten auch in Drittländer stattfinden kann, unter bestimmten Bedingungen. Aber das Papier des DSK sagt, dass eine souveräne Cloud dann vorliegt, wenn die Datenverarbeitung ausschließlich im Europäischen Wirtschaftsraum stattfindet.

00:08:07 Voget

OK, das ist auf jeden Fall super interessant und ja auch praktisch sehr relevant. Also ich meine, es gibt ja sehr viele Clouds, die sicherlich auch irgendwie Server in den USA oder in anderen Drittstaaten liegen haben und da ist das natürlich sehr wichtig, was die DSK da, zumindest momentan, für eine Auffassung vertritt. Bei mir auf der Liste finde ich jetzt auch das Kriterium der Offenheit, was ist damit gemeint?

00:08:29 Müller

Genau bei der thematische Offenheit geht es der DSK primär darum, dass einseitige Abhängigkeiten zwischen Anbietern und Anwendern vermieden werden sollen. Hierzu sollen die Anwender Wahlmöglichkeiten zwischen unterschiedlichen Cloud Angeboten haben und das bedeutet auch, dass ein späterer Wechsel des Cloud Angebots mit möglichst geringem Aufwand möglich sein soll. Und um diesem Kriterium gerecht werden zu können, ist es notwendig, dass die Cloud Angebote einfach zu ersetzen sind. Das heißt, sie müssen uns besonders den Export aller betrieblichen relevanten Daten, aber auch Objekte ermöglichen. Und der Offenheit von Cloud Angeboten kommt es zudem zugute, wenn die souveräne Cloud möglichst in allen Bereichen eine Nutzung auf Basis von offenen Standards erlaubt. Das haben wir schon gehört, das sieht man auch immer wieder durch die Stellungnahme, und das bedeutet, dass nicht nur Dateiformate, sondern auch zum Beispiel Schnittstellen und Protokollierungen auf offenen Standards basieren sollen. Und vielleicht passend dazu wird auch gesagt, dass besonders vorzugswürdig insbesondere Cloud Angebote sind, die vollständig auf Open Source Software basieren, um Anwendern so bei Bedarf einen Einblick in die Umsetzung der Cloud Plattform zu verschaffen.

00:09:30 Voget

Okay für mich klingt das total plausibel alles bislang, also dass man es möglichst transparent für den Nutzer, dass er auch sieht, was passiert da eigentlich, an wen gehen meine Daten, wie kann ich vielleicht noch Zugriff drauf nehmen, wie kann ich sie kontrollieren. Und jetzt steht bei mir noch sowas von Vorhersehbarkeit und Verlässlichkeit, kannst du vielleicht kurz sagen.

00:09:49 Müller

Ja, dabei geht es darum, dass eine souveräne Cloud natürlich auch möglichst lange in der Zukunft alle Anforderungen an eine solche Souveränität erfüllen soll und dass Anwendern die Möglichkeit gegeben wird, dies frühzeitig abschätzen zu können. Und hierzu zählt etwa auch, dass Anbieter die Anwender frühzeitig über alle wesentlichen Änderungen informieren, die sich vielleicht negativ auf die Souveränität des Angebots auslösen könnten. Und empfehlenswert ist beispielsweise ein transparentes Geschäfts- und Finanzierungsmodell der Anbieter, damit hierdurch Anwender die Möglichkeit haben, die Seriosität und auch die Rechtmäßigkeit von dem Cloud Dienst selbstständig einschätzen zu können. Genau, und damit die Weiterentwicklung von Eigenschaften für die Anwendung eines Cloud Angebots verlässlich ist, müssen diese dann in bestimmten Zyklen erfolgen, die transparent dargelegt werden.

00:10:38 Voget

Also auch wieder Transparenz und einfach nur n bisschen, dass sich Anwender auch als Kunde einfach, ja, sicher sein kann, dass der Cloud Dienst, den man nutzt, dass der ja auch noch länger existiert, dass die Daten quasi safe sind und dass der einfach in einer, sage ich mal, ordnungsgemäßen geschäftlichen Weise operiert. Klingt auch alles total nachvollziehbar für mich. Sagt denn die Stellungnahme jetzt aber auch was dazu, wie diese Kriterien geprüft werden sollen. Also wer entscheidet das und nach welchen Auslegungskriterien bestimmt sich das jetzt?

00:11:06 Müller

Genau dazu sagt die Stellungnahme am Ende noch ein bisschen was. Ob und welche der genannten Kriterien ein Cloud Angebot erfüllt, muss für Anwender natürlich prüf- und nachvollziehbar sein. Und das bedeutet, dass die Software nicht nur quasi theoretisch prüfbar ist. Sondern sie muss auch tatsächlich regelmäßig und spätestens bei einer Änderung von bestimmten Risiken überprüft werden. Und hierbei ist natürlich eine Bereitschaft der Anbieter erforderlich, an einer solchen Überprüfung auch tatsächlich aktiv mitzuwirken. Hierzu müssen die Anbieter dann selbst detaillierte Dokumentation bereitstellen, auf Nachfragen antworten oder sich auch selbst an Vor-Ort-Überprüfungen beteiligen. Besonders gut wäre es, wenn sie sich an den Zertifizierungsverfahren beteiligen, mit denen die Einhaltung der DSGVO und die Kriterien der DSK gemessen werden kann.

00:11:53 Voget

Alles klar, super. Ja, das klingt auch sinnig. Vielen, vielen Dank für diesen Überblick, schon mal. Vielleicht abschließend noch die Frage, wie relevant, oder für wie relevant hältst du denn jetzt dieses Papier der DSK zusammenfassend, also wie hoch ist die Relevanz in der Praxis.

00:12:08 Müller

Ja, ich glaube, dass die Kriterien tatsächlich eine große Hilfe in der Praxis leisten können. Also wenn sie zum Beispiel Universitäten oder andere wissenschaftliche Einrichtungen, aber auch Unternehmen im Auswahl Prozess bezüglich eines Cloud Computing Dienstes befinden, dann bieten die Kriterien wirklich eine gute Orientierungshilfe, um festzustellen, ob ein Cloud Dienst quasi die gängigen Anforderungen an Souveränität erfüllt. Und einen besonderen Mehrwert bietet das Positionspapier meiner Meinung nach vor allem insbesondere, weil wirklich eine Vielzahl von konkreten Kriterien genannt werden. Also es bleibt nicht bei abstrakten theoretischen Formulierungen, die vielleicht den bekannten Voraussetzungen DSGVO bereits entsprechend, sondern es werden wirklich konkrete Voraussetzungen genannt.

00:12:50 Voget

Ja, genau. Und ich finde die hast du auch gerade auch wenn es ein sehr komplexes theoretisches technisches Thema ist, sehr gut, beispielhaft dargelegt und nahegebracht, sodass man sich ein bisschen vorstellen kann, worauf man vielleicht auch privat oder halt, wenn man an einer Hochschule oder in einem privaten Unternehmen arbeitet, worauf man denn eigentlich muss, welchen Cloud Dienst man auswählt. Und damit war es dann heute das auch schon wieder mit unserer heutigen Folge. Ich würde sagen, da haben wir wieder einiges weggeforscht. Vielen Dank Johannes, auf jeden Fall nochmal für die Erläuterungen und Ihnen, liebe Hörerinnen und Hörer, vielen Dank fürs Einschalten und Zuhören. Bis zum nächsten Mal. Machen Sies gut.

00:13:24 Müller

Bis zum nächsten Mal!